(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 45 937 A 1**

(51) Int. Cl.[6]:
H 04 L 9/32
H 04 N 5/33
H 04 M 1/66
H 04 M 17/02
G 07 C 9/00

(21) Aktenzeichen: 196 45 937.0
(22) Anmeldetag: 7. 11. 96
(43) Offenlegungstag: 14. 5. 98

DE 196 45 937 A 1

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

(72) Erfinder:
Pfeifer, Klaus, Dipl.-Ing., 64380 Roßdorf, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

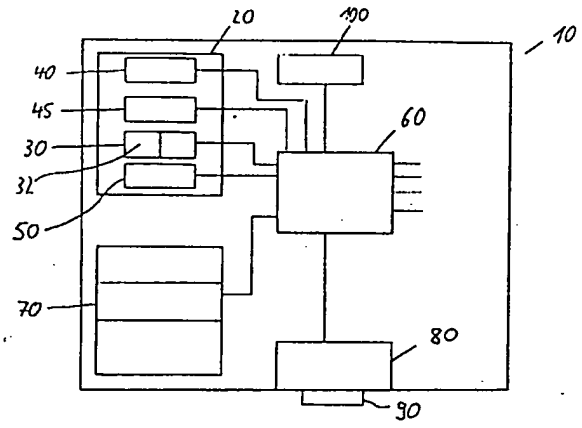
DE	43 22 445 C1
DE	43 44 481 A1
DE	42 31 913 A1
DE	34 38 106 A1
DE	33 35 678 A1
GB	22 56 170 A
US	55 57 665
US	54 69 506
US	52 28 094
US	49 93 068
US	49 91 205
EP	01 30 569 B1
EP	03 04 547 A2
JP	5-1 99 221 A

MILLER,Benjamin: Vital signs of identity. In: IEEE spectrum, Febr. 1994, H. 2, S.22-30;
Fingerabdruck wird zum Schlüssel. In: VDI nachrichten, Nr. 3, 22. Jan. 1993, S.13;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren und System zum personenabhängigen Steuern einer Telekommunikations-Endeinrichtung

(57) Die Erfindung betrifft ein Verfahren und ein System zum personenabhängigen Steuern einer zentralen Telekommunikationseinrichtung und/oder einer mit dieser verbindbaren Telekommunikations-Endeinrichtung (10). Die Erfindung kombiniert eine programmierbare Steuereinrichtung (60) mit einem Chipkartensystem (80, 90) und einer Detektoreinrichtung (30) umfassend einen biometrischen Sensor (32) zur Erfassung und Wiedererkennung von bestimmten Merkmalen aus einer menschlichen Fingerkuppe, wobei diese Komponenten der Telekommunikations-Endeinrichtung (10) zugeordnet sind. Damit läßt sich der Bedienkomfort bei der Prüfung zur Zugangsberechtigung eines Benutzers zur Telekommunikations-Endeinrichtung (10) verbessern und zusätzlich ist ein höherer Schutz gegenüber unerwünschter Fremdbenutzung gewährt.



DE 196 45 937 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zum personenabhängigen Steuern einer zentralen Telekommunikationseinrichtung, insbesondere eine TK-Anlage, eine Vermittlungsstelle u.s.w., und/oder einem mit dieser verbindbaren Telekommunikations-Endeinrichtung, insbesondere ein Telefon, eine Set-Top-Box und dergleichen, nach Anspruch 1, ein System zur Durchführung dieses Verfahrens gemäß dem Oberbegriff des Anspruchs 10, eine Schaltungsanordnung für den Einsatz in diesem System gemäß dem Oberbegriff des Anspruchs 18 sowie eine Telekommunikations-Endeinrichtung nach Anspruch 21 mit einer Schaltungsanordnung nach Anspruch 18.

Auf dem Gebiet der Telekommunikation werden Endgeräte, wie z. B. Komforttelefone, Faxgeräte oder zukünftige Set-Top-Boxen, zur Verfügung gestellt, die durch eine Zeichenkombination, auch PIN-Code genannt, für einen nicht berechtigten Benutzer gesperrt werden können. Ein derartig geschütztes Endgerät kann erst betrieben werden, wenn ein Benutzer seinen richtigen PIN-Code eingegeben hat.

Zum Schutz eines Endgerätes vor einer unberechtigten Nutzung können auch Chipkartensysteme zur Prüfung der Nutzungsberechtigung eines Benutzer eingesetzt werden, wobei die Chipkarte durch einen PIN-Code gegen Mißbrauch geschützt ist. Im Bereich der Telekommunikation gibt es Chipkartensysteme, wie z. B. Berechtigungskarten für Mobilfunkdienste, Telesec-Chipkarten, T-Card und Telefonkarten. Die bekannten Systeme zur Überprüfung von Zugangsberechtigungen sind allerdings nicht sehr benutzerfreundlich, da der Benutzer vor Nutzungsbeginn erst den richtigen Freigabe-Code eingeben muß, bevor die Endeinrichtung verfügbar ist. Das bedeutet, daß der Benutzer den PIN-Code entweder ständig im Gedächtnis behalten oder schriftlich fixiert haben muß. Ferner müssen zur Eingabe des PIN-Codes eine Folge von Tasten gedrückt werden. Darüber hinaus besteht bei der Eingabe eines PIN-Codes über eine Tastatur des jeweiligen Endgeräts die Gefahr, daß der PIN-Code während der Eingabe durch einen nicht Befugten ausgespäht werden kann.

Der Erfindung liegt daher die Aufgabe zugrunde, den Bedienkomfort zur Authentifizierung eines Benutzers gegenüber einer ein Chipkartensystem aufweisenden Telekommunikations-Endeinrichtung zu verbessern und zusätzlich einen höheren Schutz gegen unerwünschte Fremdbenutzungen zu ermöglichen.

Das technische Problem löst die Erfindung mit den Verfahrensschritten des Anspruchs 1 sowie den Merkmalen des Anspruchs 10.

Damit ein Benutzer bei seiner Authentifizierung gegenüber einer Telekommunikations-Endeinrichtung die Zeichen eines PIN-Codes nicht mehr einzeln eingeben muß, ist der Telekommunikations-Endeinrichtung eine Detektoreinrichtung zugeordnet, die bestimmte Merkmale wenigstens eines vorbestimmten menschlichen Körperteils, vorzugsweise einer Fingerkuppe, eines Benutzers erfassen und daraus eine individuelle digitale Benutzerkennung erzeugen kann. Diese aktuell gewonnene Benutzerkennung wird anschließend in einer programmierbaren Steuereinheit mit einer digitalen Referenzkennung verglichen, die zuvor aus einem kartenförmigen, tragbaren Datenträger ausgelesen worden ist. Die Referenzkennung wird aus den Merkmalen desselben Körperteils des Benutzers erzeugt, und zwar auf die gleiche Weise wie die Benutzerkennung. Die Erzeugung der digitalen Referenz- und Benutzerkennung kann je nach Systemimplementierung in ein und derselben Detektoreinrichtung oder in getrennten aber funktionsgleichen Detektoreinrichtungen erfolgen.

Eine bevorzugte Detektoreinrichtung verwendet einen an sich bekannten biometrischen Sensor, der von dem vorbestimmten menschlichen Körperteil ein Infrarot-Wärmebild aufnimmt. Ein in der Detektoreinrichtung implementiertes, an sich bekanntes Rechnerprogramm analysiert anschließend das Infrarot-Wärmebild und erzeugt anhand bestimmter Merkmale eine für jede Person eindeutige digitale Referenz- bzw. Benutzerkennung. Ein solcher biometrischer Sensor ist von der Firma BSM zusammen mit den notwendigen Analyseprogrammen entwickelt worden.

Es können auch Detektoreinrichtungen zum Einsatz kommen, die elektronische Bilder erstellen können.

Nach dem Vergleich der aus dem Datenträger ausgelesenen Referenzkennung mit der vom Benutzer aktuell gewonnenen Benutzerkennung wird in Abhängigkeit von dem Vergleichsergebnis die Telekommunikations-Endeinrichtung und/oder eine zentrale Telekommunikationseinrichtung, wie z. B. eine Vermittlungsstelle, Multimedia-Datenbank u.s.w., in vorbestimmter Weise gesteuert.

Mit Hilfe kryptographischer Schlüssel können die digitalisierte Benutzerkennung und die digitale Referenzkennung zusätzlich vor Mißbrauch weitestgehend geschützt werden. Die chiffrierten Kennungen müssen jedoch vor den Vergleichsoperationen zur Feststellung der Identität einer Benutzerkennung mit einer Referenzkennung mit dem gleichen Schlüssel wieder dechiffriert werden. Selbstverständlich sind die zum dechiffrieren erforderlichen kryptographischen Schlüssel seitens des Herstellers bzw. des Anbieters der Telekommunikations-Endeinrichtungen geheim zu halten.

Im einfachsten Fall erhält ein berechtigter Benutzer nach einem positiven Vergleichsergebnis Zugang zu allen Funktionen der Telekommunikations-Endeinrichtung und zu allen von der zentralen Telekommunikationseinrichtung zur Verfügung gestellten Diensten.

Die Erfindung sieht allerdings auch die Möglichkeit vor, berechtigten Personen definierte Nutzungsberechtigungen, die beispielsweise ihren Aufgabenstellungen oder ihrer Position im Unternehmen entsprechen, hinsichtlich der Funktionen der Telekommunikations-Endeinrichtung und/oder der zentralen Telekommunikationseinrichtung einzuräumen. Innerhalb von Familien können Eltern ihre Kinder auf die Nutzung von bestimmten Rufnummern, bestimmten Regionen oder in Abhängigkeit eines bestimmten Kostenlimits beschränken. Dazu ist eine Prüfung der Zugriffsberechtigung der Chipkarte und damit des jeweiligen Benutzers in Bezug auf die Telekommunikations-Endeinrichtung erforderlich.

Gemäß einem Ausführungsbeispiel werden zunächst in der Chipkarte wenigstens die benutzerbezogene Tabelle mit Zugriffsberechtigungen und/oder individuellen Informationen eines Benutzers (Karteninhabers) abgelegt. Bei den Zugriffsberechtigungen handelt es sich insbesondere um definierte Leistungsmerkmalen (d. h. Funktionen des Endgeräts) der Telekommunikations-Endeinrichtung und definierte Telekommunikationsdiensten, die dem Benutzer an der Telekommunuikations-Endeinrichtung von der zentralen Telekommunikationseinrichtung aus zur Verfügung gestellt werden können. Die benutzerbezogenen Zugriffsberechtigungen werden von der Steuereinrichtung zur personenabhängigen Steuerung – Freigabe und Sperren von Leistungsmerkmalen der Telekommunikations-Endeinrichtung und von Telekommunikationsdiensten, die die zentrale Telekommunikationseinrichtung bereitstellt – der Telekommunikations-Endeinrichtung und/oder der zentralen Telekommunikationseinrichtung verwendet.

Alternativ dazu können die benutzerbezogenen Tabellen mit Zugriffsberechtigungen in einer der Telekommunikati-

ons-Endeinrichtungen zugeordneten Speichereinrichtung und/oder in der zentralen Telekommunikationseinrichtung vorab abgespeichert werden.

Um jedoch eine Prüfung der Zugriffsberechtigung der Karte und somit des Karteninhabers hinsichtlich der Telekommunikations-Endeinrichtung und eine richtige Zuordnung einer benutzerbezogenen Zugriffsberechtigungs-Tabelle zu der jeweiligen berechtigten Personen bewirken zu können, muß in einem zweiten Schritt gemäß einer Ausführungsform in der der Telekommunikations-Endeinrichtung zugeordneten Speichereinrichtung und/oder in der zentralen Telekommunikationseinrichtung wenigstens die digitale Referenzkennung eines Benutzers abgespeichert werden. Nach einer positiven Authentifizierungsprüfung wird anschließend die aktuell erzeugte Benutzerkennung noch mit der oder jeder in der Speichereinrichtung und/oder in der zentralen Telekommunikationseinrichtung abgespeicherten Referenzkennung verglichen. In Abhängigkeit von diesem Vergleichsergebnis wird die benutzerbezogene Zugriffsberechtigungs-Tabelle von der Steuereinheit zur personenabhängigen Steuerung der Telekommunikations-Endeinrichtung und/oder der zentralen Telekommunikationseinrichtung verwendet.

Da das Abspeichern von zusätzlichen Referenzkennungen zur Prüfung von benutzerbezogenen Zugriffsberechtigungen ein aufwendiges Verfahren darstellt und auch aus Sicherheitsgründen bedenklich erscheint, kann vorteilhafterweise vorab in den kartenförmigen, tragbaren Datenträger wenigstens eine einem Kartenbenutzer zugeordnete Datenträgerkennung und in die, der Telekommunikations-Endeinrichtung zugeordnete Speichereinrichtung und/oder in die zentrale Telekommunikationseinrichtung wenigstens die Datenträger-Kennung(en) eines Datenträgers abgelegt werden. Vor jeder Authentifizierungsprüfung (das ist der Vergleich zwischen Referenz- und aktuell gewonnener Benutzerkennung) wird jede Datenträger-Kennung, die auf dem in der Telekommunikations-Endeinrichtung eingesetzten Datenträger gespeichert ist, mit den in der Speichereinrichtung und/oder in der zentralen Telekommunikationseinrichtung gespeicherten Datenträger-Kennungen verglichen. Bei einem positiven Vergleichsergebnis sendet die Chipkarte entsprechende Steuerdaten – das können z. B. Speicheradressen oder Benutzernamen sein – zur Telekommunikations-Endeinrichtung und/oder zentralen Telekommunikationseinrichtung. Unter Ansprechen auf die Steuerdaten liest die jeweilige Steuereinrichtung die entsprechende Zugriffsberechtigungs-Tabelle zur personenabhängigen Steuerung der Telekommunikations-Endeinrichtung und/oder der zentralen Telekommunikationseinrichtung aus der Speichereinrichtung aus. Bei einem negativen Vergleichsergebnis wird der Zugang dieser Chipkarte zur Telekommunikations-Endeinrichtung und/oder zur zentralen Telekommunikationseinrichtung durch die Steuereinrichtung unmittelbar verweigert.

Je nach Leistungsfähigkeit der einzelnen Systeme werden die Vergleichsschritte in der Telekommunikations-Endeinrichtung, der zentralen Telekommunikationseinrichtung, einer der Telekommunikations-Endeinrichtung zugeordneten Steuereinrichtung und/oder in dem tragbaren Datenträger selbst durchgeführt.

Eine zweckmäßige Weiterbildung sieht vor, bei einem negativen Vergleichsergebnis während der Authentifizierungsprüfung den Zugang zur Telekommunikations-Endeinrichtung und/oder zur zentralen Telekommunikationseinrichtung zu sperren.

Ein System zur Durchführung des oben beschriebenen Verfahrens umfaßt wenigstens eine Telekommunikations-Endeinrichtung und eine ihr zugeordnete Einrichtung zum Lesen eines kartenförmigen, tragbaren Datenträgers. Darüber hinaus ist der Telekommunikations-Endeinrichtung eine Detektoreinrichtung zum Erfassen von Merkmalen wenigstens eines vorbestimmten menschlichen Körperteils und zur Umsetzung der erfaßten Merkmale in eine digitale Benutzerkennung zugeordnet. Jeder Datenträger weist eine Speichereinrichtung auf, in der wenigstens eine digitale Referenzkennung gespeichert ist, die aus den mit Hilfe der oder einer funktionsgleichen Detektoreinrichtung erfaßten Merkmalen des vorbestimmten menschlichen Körperteils erzeugbar ist. Darüber hinaus ist jeder Telekommunikations-Endeinrichtung eine programmierbare Steuereinrichtung zum Vergleichen der digitalen Referenzkennung mit einer von der Detektoreinrichtung gewonnenen Benutzerkennung und zum Benutzer-abhängigen Steuern der Telekommunikations-Endeinrichtung in Abhängigkeit vom Vergleichsergebnis zugeordnet. Die Funktionen der Steuereinrichtung können entweder als eigenständige Einheiten oder in einer einzigen der Telekommunikations-Endeinrichtung zugeordneten programmierbaren Steuereinheit implementiert sein.

Vorteilhafte Weiterbildungen sind in den Unteransprüchen 11 bis 17 umschrieben.

Eine für den Einsatz in dem oben beschriebenen System geeignete Schaltungsanordnung ist in Anspruch 18 angegeben.

Vorteilhafte Weiterbildungen dieser Schaltungsanordnung sind in den Unteransprüchen 19 und 20 umschrieben.

Eine Telekommunikations-Endeinrichtung, insbesondere ein Telefon, mit einer Schaltungsanordnung nach einem der Ansprüche 18 bis 20 und mit einer in eine Tastatur integrierbaren Detektoreinrichtung ist ebenfalls Gegenstand der Erfindung.

Die Erfindung wird nachfolgend beispielhaft an einer Ausführungsform in Verbindung mit der beiliegenden Fig. näher erläutert.

Die Figur zeigt eine Telekommunikations-Endeinrichtung, die in unserem Beispiel ein Telefon 10 ist. Es sei angenommen, daß das Telefon 10 über eine Teilnehmer-Anschlußeinheit mit einer nicht dargestellten zentralen Telekommunikationseinrichtung, in diesem Beispiel eine Vermittlungsstelle, verbunden ist. Dem Telefon 10 ist ein Bedienfeld 20 zugeordnet, das eine Ein-/Ausschalte-Taste 40, eine Eingabetastatur 45, eine Programm-Modus-Taste 50 und eine Detektoreinrichtung 30, deren Funktions- und Wirkungsweise unten noch ausführlich beschrieben wird, aufweist. Die Detektoreinrichtung 30 umfaßt vorzugsweise einen biometrischen Sensor 32 der Firma BSM. Der biometrische Sensor 32 dient dazu, ein Infrarot-Wärmebild vorzugsweise von der Fingerkuppe eines Benutzers aufzunehmen. Speziell entwickelte Rechenprogramme sind in der Lage, aus dem aufgenommenen Infrarot-Wärmebild der Fingerkuppe des Benutzers anhand bestimmter Merkmale einen für den Benutzer eindeutigen digitalen Kennungscode zu erzeugen. In dem Telefon 10 ist ferner eine Speichereinrichtung 70 implementiert, deren Zweck und Speicherinhalt weiter unten noch erläutert wird. Darüber hinaus ist eine Chipkartenleseeinrichtung 80 in dem Telefon 10 angeordnet. Als weitere fakultative Komponenten können dem Telefon 10 ein Display 100 sowie je nach Leistungsfähigkeit Anschlüsse für eine Uhr, ein sprecherabhängiges Sprachdialogsystem, ein personenabhängiges Texterkennungssystem sowie eine Kommunikations-Anschlußeinheit zum Anschalten beispielsweise an eine a/b-Schnittstelle, an eine ISDN-S_0-Schnittstelle, an eine TK-Anlage und dergleichen zugeordnet sein. All diese Komponenten stehen mit einer programmierbaren Steuereinheit 60 in Verbindung, die für ein zuverlässiges Zusammenwirken aller Komponenten sorgt.

Nachfolgend wird die Funktionsweise der programmierbaren Steuereinheit 60 in Verbindung mit dem biometrischen Sensor 32 und einer in die Chipkartenleseeinrichtung 80 eingesetzten Chipkarte 90 anhand eines beispielhaften Szenarios ausführlich erläutert. Es sei angenommen, daß die Chipkarte 90 nur einem Benutzer A gehört. In dem Speicher der Chipkarte 90 ist neben einer Datenträger-Kennung auch die Referenzkennung des Benutzers A abgespeichert. Die Datenträger-Kennung kennzeichnet in eindeutiger Weise die Chipkarte 90 und wird, wie noch erläutert wird, von der Steuereinheit 60 dazu benutzt, um herauszufinden, ob der Benutzer A mit dieser Chipkarte Zugang zum Telefon 10 und/oder zur Vermittlungsstelle hat oder nicht. Die digitale Referenzkennung wird entweder mit Hilfe der Detektoreinrichtung 30 oder einer getrennten aber funktionsgleichen Einrichtung erzeugt. Wie bereits erwähnt, umfaßt die Detektoreinrichtung 30 den biometrischen Sensor 32, der aus bestimmten Merkmale eines bestimmten Körperteils des Benutzers A, vorzugsweise einer Fingerkuppe, ein Infrarot-Wärmebild erstellt, aus dem die Detektoreinrichtung 30 in Verbindung mit einem an sich bekannten Rechenprogramm die für den Benutzer A spezifische digitale Referenzkennung erzeugt. Die so für den Benutzer A gewonnene digitale Referenzkennung wird in der Chipkarte 90 abgelegt. Selbstverständlich können mehrere Chipkarten für unterschiedliche Benutzer existieren. Je nach Anwendungsfall ist es denkbar, eine Chipkarte auch mehreren Benutzern zuzuordnen. In diesem Fall müssen die entsprechenden Referenzkennungen der verschiedenen Benutzer in der Chipkarte gespeichert werden.

Vor dem erstmaligen Betrieb des Telefons 10 wird wenigstens eine Datenträger-Kennung, in unserem Beispiel ist dies die Datenträger-Kennung der Chipkarte 90, in die Speichereinrichtung 70 geschrieben. Darüber hinaus werden in die Speichereinrichtung 70 mehrere Zugriffsberechtigungs-Tabellen für verschiedene Benutzer, so auch für den Benutzer A, unter definierten Adressen abgelegt. Die richtige Verknüpfung eines berechtigten Benutzer mit der dazugehörenden Zugriffsberechtigungs-Tabelle kann über die in der Speichereinrichtung 70 abgelegte Datenträger-Kennung und deren Speicheradresse erfolgen. In jeder Zugriffsberechtigungs-Tabelle stehen definierte Leistungsmerkmale des Telefons 10, zu denen die jeweiligen Benutzer Zugang haben. Beispielhafte Leistungsmerkmale des Telefons 10 sind:

1. Durch eine Auswertung der vom Nutzer eingegebenen Zielrufnummer können durch die programmierte Steuereinheit 60 gewünschte Beschränkungen zugänglicher Telekommunikationsdienste erfolgen:
   - Bei Eingabe einer 0 an der ersten Stelle der Zielwahlrufnummer kann durch eine Sperrung der weiteren Funktionen eine Beschränkung der Telekommunikationsmöglichkeiten auf das lokale Ortsnetz oder eine TK-Anlage bewirkt werden,
   - bei der Eingabe einer 0 an der zweiten Stelle der Zielwahlrufnummer kann, wenn die erste Stelle ebenfalls eine 0 war, durch eine Sperrung der weiteren Funktionen eine Beschränkung auf das nationale Telekommunikationsnetz oder das lokale Ortsnetz bei TK-Anlagen bewirkt werden,
   - bei der Wahl von bestimmten vorgegebenen Rufnummer können in diesen Einzelfällen die zuvor genannten Beschränkungen außer Kraft gesetzt werden,
   - bei der Wahl von bestimmten Telekommunikations-Dienstezugangsrufnummern, wie z. B. 0190, kann eine Beschränkung erfolgen, die diese für den Nutzer sperrt oder nur für eine bestimmte Zeitdauer erlaubt.
2. Durch eine nutzerabhängige Addierung der anfallenden Telekommunikationskosten können durch die Vorgabe eines Kostenlimits, welches auch auf Zeitintervalle bezogen werden kann, bei Erreichen dieses Kostenlimits Beschränkungen wirksam werden.
3. Durch Anwendung von zeitlichen Kriterien können definierte Benutzerberechtigungen sich über den Tages-, Wochen- oder Datumsverlauf ändern.
4. Bei entsprechenden Speicherfaxgeräten können berechtigte Personen, deren Authentität über die Steuereinheit 60 festgestellt wird, eingegangene und abgespeicherte Faxnachrichten ausdrucken oder auf andere Datenträger überspielen.
5. Bei entsprechend ausgestatteten Set-Top-Boxen können für als berechtigt erkannte Nutzer der Abruf und die Entschlüsselung von entsprechenden TV-, Hörfunk- und sonstigen Programmen, wie z. B. Multimedia-Spiele, Tele-Shopping-Formen, nach bestimmten individuellen Kriterien, wie z. B. Preis- bzw. Kostengrenzen oder zeitlichen Kriterien, gesteuert werden.

Um die entsprechenden Tabellen und Datenträger-Kennungen in die Speichereinrichtung 70 einschreiben zu können, wird die Steuereinheit 60 über die Programm-Modus-Taste 50 in den Programmier-Modus gesetzt. Der Zugang zum Programmier-Modus ist vorteilhafterweise durch einen PIN-Code gesichert. Der Programmier-Modus ermöglicht ferner die Erfassung, Digitalisierung, Umsetzung und Abspeicherung von Referenzkennungen bestimmter Benutzer auf den Chipkarten. Die Ausführung und Gestaltung des Programmier-Modus und der Steuereinheit 60 hängen jedoch wesentlich von den Funktionen der jeweiligen Telekommunikations-Endeinrichtung (z.B: Telefon oder Set-Top-Box) ab.

Nach dieser Vorbereitungsprozedur kann das Telefon mittels der Ein-/Ausschalte-Taste 40 eingeschaltet werden. Nach dem Einschalten startet die Steuereinheit 60 automatisch den Retriebsmodus, der mit dem Authentifizierungsvorgang zu Prüfung des berechtigten Karteninhabers und damit der Zugangsberechtigung des Benutzers A zum Telefon 10 beginnt. Die Steuereinheit 60 kann derart programmiert sein, daß der Benutzer A unmittelbar nach dem Einschalten des Telefons 10 im Display 100 zum Einstecken der Chipkarte 90 in die Chipkarten-Leseeinrichtung 80 und danach zur Kontaktierung der Fingerkuppe des Referenzfingers mit dem biometrischen Sensor 32 aufgefordert wird. Zur Erfassung der jeweiligen biometrischen Merkmale aus der Fingerkuppe des Benutzers A weist das Bedienfeld 40 eine Taste oder ein Feld mit dem biometrischen Sensor 32 auf. Das Oberflächenprofil der Taste oder des Feldes mit dem integrierten Sensor 32 sollte eine Auswölbung aufweisen, die der Rundung der Fingerkuppe optimal angepaßt ist. Vorteilhafterweise kann die Ein-/Ausschalte-Taste mit dem Infrarot-Wärmebild-Sensor 32 ausgestattet sein. Dadurch ist es möglich, daß während der Betätigung der Ein-/Ausschalte-Taste 40 sowohl eine Inbetriebnahme des Telefons 10 als auch eine sichere Erfassung der Epidermis der aufgelegten Fingerkuppe des Benutzers A erfolgen kann. Der Sensor 32 nimmt nunmehr die biometrischen Merkmale der Fingerkuppe des Benutzers A auf. Aus diesen Merkmalen wird anschließend nach einem bekannten Verfahren die dazugehörige digitale Benutzerkennung des Benutzers A, auch Warm-Code genannt, erzeugt. Die Steuereinheit 60 ist nun derart programmiert, daß sie die auf der Chipkarte 90 abgespeicherte digitale Referenzkennung ausliest und mit der digitalen Benutzerkennung des aktuellen Benutzers A vergleicht. Obwohl in diesem Beispiel die programmierbare

Steuereinheit 60 integraler Bestandteil des Telefons 10 ist, kann eine ähnliche Steuereinheit auch in der Chipkarte 90, beispielsweise in einem Gehäuse separat zum Telefon 10 oder sogar in der Vermittlungsstelle angeordnet sein. Mit anderen Worten ist es nicht notwendig, daß das Vergleichsprogramm in der Steuereinheit 60 des Telefons 10 durchgeführt wird. Um die jeweiligen Kennungen gegen Mißbrauch zu schützen, kann sowohl die Referenzkennung als auch die Benutzerkennung mit Hilfe eines öffentlichen Schlüssels (RSA-Chiffrier-Schlüssel) chiffriert werden. In diesem Fall werden die chiffrierten Kennungen vor dem Vergleichen mit dem gleichen Schlüssel wieder dechiffriert.

In Abhängigkeit des Vergleichsergebnisses erfolgt durch die Steuereinheit 60 die weitere Steuerung des Telefons 10 und/oder der Vermittlungsstelle. Wenn keine identische Übereinstimmung oder keine Übereinstimmung in einem vorgegebenen Toleranzbereich zwischen der aus der Chipkarte 90 ausgelesenen Referenzkennung und der aktuellen Benutzerkennung festgestellt wird, wird aufgrund der nicht festgestellten Authentität des Chipkartennutzers A eine weitergehende Benutzung des Telefons 10 beispielsweise durch Sperrung der Eingabetastatur 45 verhindert. Im Display 100 des Telefons 10 können entsprechende Hinweise, wie z. B. "Es besteht keine Nutzerberechtigung" oder auch "Bitte richtigen Tastfinger verwenden" angezeigt werden. Wird jedoch eine identische Übereinstimmung oder eine Übereinstimmung in einem vorgegebenen Toleranzbereich zwischen der Referenzkennung und der Benutzerkennung festgestellt, d. h. der Benutzer A der Chipkarte 90 ist als berechtigte Person identifiziert worden, muß zwischen zwei Alternativen unterschieden werden. Nach der ersten Alternative verfügt der berechtigte Benutzer A Zugang zu allen Leistungsmerkmalen des Telefons 10 und zu allen zur Verfügung stehenden Telekommunikationsdienstleistungen. Gemäß der zweiten Alternative wird vorteilhafterweise vor der Authentifizierung des Benutzers A gegenüber der Chipkarte 90 noch geprüft, ob der Benutzer A mit seiner Chipkarte 90 überhaupt eine Zugangsberechtigung zum Telefon 10 besitzt und in welchem Umfang. Dazu sind, wie bereits erwähnt, in der Chipkarte 90 neben der Referenzkennung des Karteninhabers A die Datenträger-Kennung, wenigstens die Datenträger-Kennung der Chipkarte 90 in der Speichereinrichtung 70 des Telefons 10 und/oder in der Vermittlungsstelle und wenigstens die Zugriffsberechtigungstabelle eines Benutzers (in unserem Beispiel die des Benutzers A) in der Speichereinrichtung 70 des Telefons 10 und/oder der Vermittlungsstelle abgelegt. Bevor sich der Karteninhaber A gegenüber seiner Chipkarte 90 authentifizieren muß, liest die Steuereinheit 60 die Datenträger-Kennung aus der eingesetzten Chipkarte 90 aus und vergleicht sie mit den in der Speichereinrichtung 70 abgelegten Datenträger-Kennungen und prüft, ob die eingesetzte Chipkarte 90 und damit der Benutzer A eine Zugangsberechtigung zu dem Telefon 10 hat. Wenn die Datenträger-Kennung der eingesetzten Chipkarte 90 in der Speichereinrichtung 70 enthalten ist, wird der Benutzer beispielsweise über einen Hinweis in dem Display 100 aufgefordert, sich mit seinem Fingerabdruck gegenüber der Chipkarte 90 zu authentifizieren, wie dies bereits oben ausführlich beschrieben worden ist. Nach einer positiven Authentifizierung sendet beispielsweise die Chipkarte 90 eine Adresse zur Steuereinrichtung 60, unter der die dazugehörige Zugriffsberechtigungs-Tabelle des Karteninhabers A in der Speichereinrichtung 70 zu finden ist. Die Steuereinrichtung 60 liest diese Tabelle aus und übernimmt sie in ihr Steuerprogramm. In Abhängigkeit des Inhaltes der ausgelesenen Zugriffsberechtigungs-Tabelle werden die entsprechenden Leistungsmerkmale des Telefons 10 sowie die Telekommunikationsdienste, die die Vermittlungsstelle dem Benutzer bereitstellt, aktiviert oder deaktiviert. Es ist auch denkbar, die Zugriffsberechtigungs-Tabelle des Benutzers A auf der Chipkarte 90 abzuspeichern, auf die die Steuereinheit 60 im Falle eines positiven Vergleichsergebnisses zugreifen kann. Der Zugang des Benutzers A zu dem Telefon 10 kann nachträglich dadurch verhindert werden, daß die entsprechende Datenträger-Kennung in der Speichereinrichtung 70 gelöscht wird. Die Prüfung der Zugangsberechtigung der Chipkarte 90 zum Telefon 10 kann auch nach der Authentifizierungsprüfung durchgeführt werden. Dank der Verwendung der Chipkarte 90 ist es möglich, dem Benutzer A bestimmte Zugriffsberechtigungen zu erteilen, ohne seine Referenzkennung in dem Telefon 10 oder der Vermittlungsstelle hinterlegen zu müssen.

Anstatt in jeder Chipkarte eine Datenträger-Kennung und in dem Telefon 10 bzw. der Vermittlungsstelle wenigstens eine Datenträger-Kennung abzulegen, können in die Speichereinrichtung 70 des Telefons 10 und/oder in die Vermittlungsstelle wenigstens die Referenzkennung eines Benutzers abgelegt werden, die zur Überprüfung der Nutzungsberechtigung der Chipkarte 90 in bezug auf das Telefon 10 benutzt wird. Allerdings wird in der Praxis wohl die erste Lösungsvariante bevorzugt werden, da die zweite Lösungsvariante es erforderlich macht, daß von jedem möglichen Benutzer eine digitale Referenzkennung einer vorbestimmten Fingerkuppe mit Hilfe eines biometrischen Sensor aufgenommen, digitalisiert und dann in die Speichereinrichtung 70 bzw. in die Vermittlungsstelle abgelegt wird.

Zur Erhöhung der Authentifikationssicherheit eines berechtigten Benutzers gegenüber seiner Chipkarte, beispielsweise wenn die Referenz-Fingerkuppe wegen einer Verletzung nicht benutzt werden kann, können von dem Benutzer auch mehrere Referenzkennungen von verschiedenen Fingerkuppen erfaßt und auf der Chipkarte gespeichert werden.

Durch zusätzliche Verknüpfung von zwei Referenzkennungen und der Abfrage mit den zwei entsprechenden Referenzfingern kann nach Bedarf der Sicherheitspegel der Anwendung noch erhöht werden, d. h. nur wenn die beiden richtigen Fingerkuppen identifiziert wurden, wird die weitere Nutzung des Systems unterstützt.

Zur Erhöhung der Einsatzmöglichkeiten von Chipkarten können mehrere Datenträger-Kennungen abgespeichert werden, die für unterschiedliche Endgeräte-Anwendungen vorgesehen sein können.

Das oben beschriebene System ist auch dafür bestimmt, daß mehrere Personen eine Chipkarte nutzen und diese nach Bedarf untereinander austauschen können. Hierzu sind die entsprechenden Referenzkennungen der jeweiligen Fingerkuppen der vorgesehenen Personen auf der entsprechenden Chipkarte abzuspeichern. Durch eine entsprechende Verknüpfung der Speicheradressen der jeweiligen Referenzkennungen, die bei der Authentifikationsprüfung von der Steuereinheit 60 ermittelt wird, mit den den einzelnen Personen zugeordneten Datenträger-Kennungen der jeweiligen Chipkarte, können Personen-individuelle Leistungsmerkmale der berechtigten Chipkartennutzer an dem Telefon 10 realisiert werden.

Das Zusammenwirken der Steuereinheit 60 mit dem Chipkartensystem 80, 90 und dem biometrischen Sensor 32 zur Erfassung und Wiedererkennung von bestimmten Merkmalen aus der menschlichen Fingerkuppe betriebenen Telekommunikations-Endeinrichtungen bietet einen höheren Bedienkomfort und zusätzlich einen höheren Schutz gegenüber unerwünschten Fremdbenutzungen und ermöglicht außerdem den berechtigten Benutzern die individuelle Nutzung des Telefons 10 und der damit erreichbaren Telekommunikationsdienste.

Berechtigte Nutzer können definierte Nutzungsmöglich-

keiten erhalten, wodurch der Mißbrauch durch eine uneingeschränkte Nutzung vorhandener Endgeräten wesentlich eingedämmt wird.

Patentansprüche

1. Verfahren zum personenabhängigen Steuern einer zentralen Telekommunikationseinrichtung und/oder einer mit dieser verbindbaren Telekommunikations-Endeinrichtung mit folgenden Verfahrensschritten:

a) ein kartenförmiger, tragbarer Datenträger wird in eine der Telekommunikations-Endeinrichtung zugeordnete Kartenleseinrichtung eingesetzt, wobei vorab in den Datenträger wenigstens eine digitale Referenzkennung, die aus den, mit Hilfe einer Detektoreinrichtung erfaßten Merkmalen eines vorbestimmten menschlichen Körperteils, insbesondere einer Fingerkuppe, gewonnen wird, abgelegt wird;

b) die Merkmale des vorbestimmten Körperteils eines Benutzers werden von einer der Telekommunikations-Endeinrichtung zugeordneten Detektoreinrichtung, die mit der Detektoreinrichtung in Schritt a) übereinstimmt oder funktionsgleich ist, abgetastet und in eine digitale Benutzerkennung umgesetzt;

c) die Benutzerkennung wird mit der im Datenträger abgelegten Referenzkennung verglichen und

d) in Abhängigkeit von dem Vergleichsergebnis wird die Telekommunikations-Endeinrichtung und/oder die zentrale Telekommunikationseinrichtung in vorbestimmter Weise gesteuert.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Detektoreinrichtungen biometrische Sensoren enthalten, die ein Infrarot-Wärmebild von dem vorbestimmten menschlichen Körperteil aufnehmen.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die digitalisierte Benutzerkennung und die digitalisierte Referenzkennung kryptografisch verschlüsselt und vor Ausführung des Schrittes c) kryptografisch dechiffriert werden.

4. Verfahren nach Anspruch 1, 2 oder 3, dadurch gekennzeichnet, daß im Datenträger wenigstens eine Benutzer-bezogene Tabelle mit Zugriffsberechtigungen insbesondere zu definierten Leistungsmerkmalen abgelegt wird, die in Schritt d) zur personenabhängigen Steuerung der Telekommunikations-Endeinrichtung und/oder der zentralen Telekommunikationseinrichtung verwendet wird.

5. Verfahren nach Anspruch 1, 2 oder 3, dadurch gekennzeichnet, daß in einer der Telekommunikations-Endeinrichtung zugeordneten Speichereinrichtung und/oder in der zentralen Telekommunikationseinrichtung vorab wenigstens eine Benutzer-bezogene Tabelle mit Zugriffsberechtigungen insbesondere zu definierten Leistungsmerkmalen abgespeichert werden, die in Schritt d) zur personenabhängigen Steuerung der Telekommunikations-Endeinrichtung und/oder der zentralen Telekommunikationseinrichtung verwendet wird.

6. Verfahren nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß vorab in den Datenträger eine Datenträger-Kennung und in die der Telekommunikations-Endeinrichtung zugeordnete Speichereinrichtung und/oder in die zentrale Telekommunikationseinrichtung wenigstens die Datenträger-Kennung eines Datenträgers abgelegt werden, daß vor Ausführung des Schritts c) die Datenträgerkennung, die auf dem in der Telekommunikations-Endeinrichtung eingesetzten Datenträger gespeichert ist, mit der in der Speichereinrichtung und/oder in der zentralen Telekommunikationseinrichtung gespeicherten Datenträger-Kennung verglichen wird und daß bei einem negativen Vergleichsergebnis der Zugang zur Telekommunikations-Endeinrichtung und/oder der zentralen Telekommunikationseinrichtung gesperrt wird.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß nach einem positiven Vergleich in Schritt c) die Chipkarte Steuerdaten zur Telekommunikations-Endeinrichtung und/oder zur zentralen Telekommunikationseinrichtung aus sendet und daß in Abhängigkeit von den Steuerdaten die zugehörende Zugriffsberechtigungs-Tabelle zur personenabhängigen Steuerung der Telekommunikations-Endeinrichtung und/oder der zentralen Telekommunikationseinrichtung verwendet wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß die Vergleichsschritte in der Telekommunikations-Endeinrichtung, der zentralen Telekommunikationseinrichtung, einer der Telekommunikations-Endeinrichtung zugeordneten Steuereinrichtung und/oder dem tragbaren Datenträger durchgeführt werden.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß bei einem negativen Vergleichsergebnis in Schritt c) der Zugang zur Telekommunikations-Endeinrichtung und/oder zur zentralen Telekommunikationseinrichtung gesperrt wird.

10. System zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 9, umfassend wenigstens eine Telekommunikations-Endeinrichtung (10) und wenigstens einen kartenförmigen, tragbaren Datenträger (90) dadurch gekennzeichnet, daß der Telekommunikations-Endeinrichtung (10) eine Kartenleseeinrichtung (80) und eine Detektoreinrichtung (30, 32) zum Erfassen von Merkmalen wenigstens eines vorbestimmten menschlichen Körperteils und zur Umsetzung der erfaßten Merkmale in eine digitale Benutzerkennung zugeordnet sind, daß der tragbare Datenträger (90) eine Speichereinrichtung aufweist, in der wenigstens eine digitale Referenzkennung, die aus den, mit Hilfe der oder einer funktionsgleichen Detektoreinrichtung erfaßten Merkmalen des vorbestimmten menschlichen Körperteils erzeugbar ist, gespeichert ist und daß der Telekommunikations-Endeinrichtung (10) eine programmierbare Steuereinrichtung (60) zum Vergleichen der digitalen Referenzkennung mit einer von der Detektoreinrichtung (30, 32) gewonnenen Benutzerkennung und zum Benutzer-bezogenen Steuern der Telekommunikations-Endeinrichtung in Abhängigkeit vom Vergleichsergebnis zugeordnet ist.

11. System nach Anspruch 10, dadurch gekennzeichnet, daß jede Detektoreinrichtung (30) wenigstens einen biometrische Sensor (32) enthält, die ein Infrarot-Wärmebild von dem vorbestimmten menschlichen Körperteil, insbesondere einer Fingerkuppe aufnehmen.

12. System nach Anspruch 10 oder 11, dadurch gekennzeichnet, daß der tragbare Datenträger (90) eine programmierbare Steuereinrichtung aufweist.

13. System nach Anspruch 12, gekennzeichnet durch eine mit der Telekommunikations-Endeinrichtung (10) verbindbaren, zentralen Telekommunikationseinrichtung, wobei in der Speichereinrichtung des Datenträgers (90) eine Datenträger-Kennung gespeichert ist und in einer der Telekommunikations-Endeinrichtung (10)

zugeordneten Speichereinrichtung (70) und/oder in der zentralen Telekommunikationseinrichtung wenigstens die Datenträger-Kennung eines tragbaren Datenträgers (90) ablegbar ist.

14. System nach einem der Ansprüche 10 bis 13, dadurch gekennzeichnet, daß jede Steuereinrichtung zum Vergleichen einer in der jeweiligen Speichereinrichtung (70) enthaltenen Datenträger-Kennung mit der Datenträger-Kennung des Datenträgers (90), der in der Telekommunikations-Endeinrichtung (10) eingesetzt ist, ausgebildet sein kann.

15. System nach einem der Ansprüche 10 bis 14, gekennzeichnet durch wenigstens eine Benutzer-bezogene Tabelle mit Zugriffsberechtigungen insbesondere zu definierten Leistungsmerkmalen, die in der der Telekommunikations-Endeinrichtung (10) zugeordneten Speichereinrichtung (70), in der zentralen Telekommunikationseinrichtung und/oder im tragbaren Datenträger (90) gespeichert ist.

16. System nach einem der Ansprüche 10 bis 15, dadurch gekennzeichnet, daß der Telekommunikations-Endeinrichtung (10) eine Tastatur (45), ein Display (100), ein Sprecher-abhängiges Sprachdialogsystem, ein Zeitgeber und/oder ein personenabhängiges Texterkennungssystem zugeordnet ist.

17. Schaltungsanordnung für den Einsatz in einem System nach einem der Ansprüche 10 bis 16, dadurch gekennzeichnet, daß die Schaltungsanordnung einer Telekommunikations-Endeinrichtung (10) zugeordnet ist und umfaßt:

eine Kartenleseeinrichtung (80),

eine Detektoreinrichtung (30, 32) zum Erfassen von Merkmalen wenigstens eines vorbestimmten menschlichen Körperteils und zur Umsetzung der erfaßten Merkmale in eine digitale Benutzerkennung,

eine programmierbare Steuereinheit (60) zum Vergleichen einer in einem kartenförmigen tragbaren Datenträger (90) gespeicherten, digitalen Referenzkennung mit einer von der Detektoreinrichtung (30, 32) gewonnenen Benutzerkennung und zum Benutzer-bezogenen Steuern der Telekommunikations-Endeinrichtung (10) in Abhängigkeit vom Vergleichsergebnis.

18. Schaltungsanordnung nach Anspruch 17, dadurch gekennzeichnet, daß die Detektoreinrichtung (30) wenigstens einen biometrischen Sensor (32) enthält, der ein Infrarot-Wärmebild von dem vorbestimmten menschlichen Körperteil, insbesondere einer Fingerkuppe aufnehmen kann.

19. Schaltungsanordnung nach Anspruch 17 oder 18, gekennzeichnet durch eine Speichereinrichtung (70) zum Ablegen wenigstens einer Benutzer-bezogenen Tabelle mit Zugriffsberechtigungen insbesondere zu Leistungsmerkmalen einer anschaltbaren Telekommunikations-Endeinrichtung (10), wenigstens einer digitalen Referenzkennung, die aus den, mit Hilfe einer Detektoreinrichtung erfaßten Merkmalen des vorbestimmten menschlichen Körperteils (Fingerkuppe) gewonnen wird, und/oder wenigstens der Datenträger-Kennung eines Datenträgers (90).

20. Telekommunikations-Endeinrichtung, insbesondere ein Telefon, mit einer Schaltungsanordnung nach einem der Ansprüche 17 bis 19, wobei die Detektoreinrichtung (30, 32) in eine Tastatur (45) integrierbar ist.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 196 45 937 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 14. Mai 1998